

Проблеми інформаційної безпеки в соціальних мережах



Горова Світлана Валеріївна –

старший науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, кандидат наук із соц. комун.

У статті тезово розглядаються основні проблеми, пов'язані із актуалізацією проблем інформаційної безпеки, у зв'язку зі зростаючою роллю соціальних мереж у процесі розвитку інформатизації українського суспільства.

Ключові слова: інформаційна безпека, інформаційні технології, інформаційний вплив, соціальні мережі, кіберзлочинність.

Постановка проблеми. Розглядаються основні напрями розвитку технологій протидії інформаційній злочинності, що проникає у вітчизняну інфосферу через комунікації соціальних мереж.

Аналіз останніх досліджень і публікацій. Розробкою питань інформаційної безпеки займаються вітчизняні та зарубіжні науковці, а саме: В. М. Бутузов, В. Д. Гавловський, В. М. Горовий, В. М. Петрик, М. М. Присяжнюк, В. В. Остроухов, О. С. Онищенко, В. С. Цимбалюк, О. М. Юрченко та інші, проте сучасний стрімкий розвиток інформаційного суспільства постійно дає новий матеріал для науково-практичних узагальнень.

Актуальність дослідження обумовлена зростанням суспільної важливості національної інформаційної безпеки в умовах глобальної інформатизації.

Метою статті є визначення основних напрямів протидії інформаційним загрозам у контексті розвитку соціальних мереж.

Виклад основного матеріалу. Сьогодні інформатизація як технологічна основа активізації глобальних процесів у всіх регіонах світу не лише забезпечує доступ усім категоріям членів сучасного суспільства до його інформаційних ресурсів, але й також залучає їх до активної участі в інформаційних обмінах, до масового розвитку процесів інфотворення. При цьому

процес створення глобального інформаційного суспільства обумовлює формування єдиного інформаційного простору, який на сучасному етапі активно впливає на соціум. Раніше, до розвитку сучасних кібернетичних систем, розуміння інформаційного простору зводилося до атмосфери, стратосфери, космосу, водних акваторій океанів і морів. Нині воно включає ще й кібернетичні та віртуальні системи. На сьогодні, розглядаючи вплив інформаційного простору на особистість, слід ураховувати, що він поширюється на суспільство та державу і через них опосередковано на кожного індивідуума [1].

Інформаційні технології сучасності сприяють зростанню соціальної активності членів суспільства. Ця активність виражається нині в реалізації можливостей для самовираження, обміну соціальним досвідом, для діяльності, спрямованої на особисте вдосконалення і внесення того чи іншого вкладу в розвиток суспільства. Особливо яскраво це проявляється при використанні технологій соціальних мереж.

Перенесення процесу утвердження соціальних інтересів у віртуальний простір призвело до суттєвих корективів у традиційному розумінні функціонування механізмів інформаційних обмінів у суспільстві. Серед найважливіших характеристик даного процесу слід зазначити наступне: по-перше, відбувається постійне зростання потужності інформаційних потоків, що значно ускладнює процес їх контролю з точки зору інформаційної безпеки. По-друге, з'явилися нові види електронних комунікацій, що поєднують у собі одночасно індивідуальні та масові характеристики впливів, у той час як традиційні технології інформаційного контролю були зорієнтовані або на індивідуальних, або на масових користувачів. По-третє, демократизація суспільства за своїм змістом не відповідає застосовуванню старих методик контролю. І, по-четверте, поки що державні системи контролю не можуть вчасно і в повній мірі реагувати на змінні, динамічні показники в інформаційному просторі [2].

При цьому, постійно зростаюча популярність соціальних мереж обумовила підвищену увагу дослідників до їх сутності та суспільного значення, оскільки лише усталені поняття про суспільне явище дають можливість перейти від фіксації особливостей того чи іншого процесу в його стихійному розвитку до управління перспективами цього розвитку.

Слід зазначити, що в умовах поширення Інтернет-технологій створення соціальних мереж стало розглядатись багатьма дослідниками

як додатковий інструмент сприяння становленню і розвитку громадянського суспільства та демократії. Адже, як слушно зазначає С. І. Даниленко, “комунікаційний простір мережі Інтернет, з позицій теорії та практики відкритого демократичного суспільства, є невід’ємною частиною громадської сфери, відкритої для всіх членів суспільства, як для публічних дебатів, так і для обміну думками між громадянськи активними індивідуумами, групами й спільнотами” [3].

Останніми роками в Україні розкриттю окремих аспектів функціонування соцмереж у контексті зміцнення засад громадянського суспільства присвячено дослідження і напрацювання таких учених, як С. І. Даниленко [3], А. М. Готун [4], О. В. Маліс [5], Є. Пілат [6] та ін.

Зокрема, в дослідженні С. І. Даниленка охарактеризовано політико-революційний потенціал глобальних соціальних мереж і їх національних сегментів, а також мережеві соціальні медіа як систему організації суспільного життя, їх місце та роль у процесі соціально-політичної соціалізації. О. В. Маліс звертає увагу на те, що мережеве співтовариство досить слабо інтегроване в реальну політичну систему і поява досконаліших технологій, що сприяють включенню громадян у політику, ще не забезпечила прямого мережевого представництва інтересів і розвитку кібердемократії в українському суспільстві. Є. Пілат, у свою чергу, розглядає соціальні мережі як фактор розвитку громадянського суспільства.

Паралельно з цим набуває розвитку цільове призначення мереж з використанням специфічних маніпулятивних технологій. Серед великого різноманіття способів інформаційних впливів, які реалізуються в інформаційному просторі або через нього, можна виділити такі: поширення спеціально підібраної інформації (дезінформації). Цей спосіб впливів здійснюється у формі: розсилки e-mail (електронних листів); організації новинних груп у соціальних мережах; створення сайтів з елементами інтерактивної взаємодії їх відвідувачів (чати, оп-line-голосування); розміщення інформації на приватних за змістом веб-ресурсах: у блогах, соціальних мережах [7].

Інформаційне маніпулювання із застосуванням різноманітних технологій інформаційно-психологічного впливу, в тому числі й сугестивних, з розвитком технологій стає все більш дієвим. Зокрема, це стосується механізмів реалізації політичного впливу. Сугестивні технології все більш активно використовуються в Інтернет-просторі та набувають масштабів, що співвідносяться із загрозами для національного інформаційного простору. Слід зазначити, що під сугестією розуміють форму міжособистісного й міжгрупового спілкування, при якому передання інформації відбувається за допомогою частково неусвідомлюваного, направлено сигналу на вербальному чи невербальному рівнях. Сугестія відрізняється від переконання зниженням рівнем критичності й потреби у верифікації інформації. Особливо ефективні такі технології в Інтернеті з певних причин: по-перше, все ще існує висока

довіра до неофіційних ресурсів мережі. По-друге, аудиторія може бути залучена до інформації обіцянкою розв’язати будь-які проблеми. По-третє, формування мережевих співтовариств на основі емпатії (співчуття). Сугестивні технології можуть торкатися нервово-психічних процесів і соціальних уявлень, настанов, суспільних норм, цінностей, думок, а також індивідуальної самосвідомості відвідувачів інтернетних ресурсів. Відповідно, сугестивний вплив на мережеві співтовариства може спонукати їхніх представників до певних дій у реальному світі [8].

Варто також зауважити, що діяльність сучасних кіберзлочинців стала також досить серйозним бізнесом: вони залучають зовнішніх співробітників (аутсорсерів) – талановитих програмістів, створюють програмні продукти і пропонують платні послуги, отримують прибутки. Соціальні мережі, на думку фахівців, знаходяться в числі найбільш уразливих для атак злочинців поряд із Інтернет-платежами, Інтернет-банкінгом; віддаленими сховищами даних і програмних застосувань; онлайновими іграми; онлайновими біржовими агенціями; сайтами за технологіями Web 2.0. [9].

Можливості технологій соціальних мереж вносять нові корективи і в уявлення про інформаційну безпеку. Особисті дані користувачів, що знаходяться в загальному доступі, можуть бути використані без дозволу в рекламних цілях, з вини мережі може бути здійснено витік платіжних даних. Серйозні неприємності для користувача можуть бути пов’язані зі зломом акаунта і використанням всієї інформації для шкоди йому, в тому числі з метою політичного чи економічного шпигунства, дискредитації та ін. дій з метою помсти. Загрозливим є так званий фішинг, вірус, що непомітно для користувача краде його логін і пароль, а потім використовує їх для автоматичної розсилки спаму від імені користувача по всьому списку його контактів [10].

Спеціалісти зауважують, що соціальні мережі, які активно розширюються, стають каналом для надання суб’єктом впливу потрібної йому інформації. При цьому він має можливість формувати чітку диференціацію об’єктів впливу та охоплення масштабних аудиторій, зменшувати здатності об’єкта впливу блокувати інформацію, організовувати протидію в інформаційній сфері не тільки проти визнаних ворогів, але й проти задекларованих партнерів як на міждержавному рівні (наприклад, союзники по коаліції чи блоку), так і у політичній чи бізнесовій площині (політичні блоки, бізнес-асоціації тощо) [11].

Соціальні мережі, не зважаючи на те, що в практику спілкування ввійшли лише протягом останніх 5–7 років, стали вже важливим інструментом активізації горизонтального спілкування як основи для організації соціальних протестів, як таких, що сприяють удосконаленню суспільної організації, так і тих, що в силу емоційного впливу і некритичного ставлення до реального життя за межами комп’ютерних спільнот, про-

являються у вигляді деструктивних виступів, використовуються внутрішніми та іноземними кукловодами для вирішення цілей, не пов'язаних із національним прогресом.

І, нарешті, аналіз уже існуючого суспільного досвіду свідчить, що соціальні мережі, з наявним ресурсом соціальної довіри, обумовленою слабкою присутністю на даному етапі розвитку в їх інформаційних впливах державних органів і традиційних політичних сил, наразі досить успішно використовуються для просування власних інтересів не лише сферою бізнесу, але й іншими суб'єктами впливу для введення в суспільний обіг тенденційної, або ж просто шкідливої для об'єкта впливу інформації. Вони, як про це свідчать події останніх років, можуть ставати ефективним інструментом інформаційних воєн і складовим елементом локальних воєн й військових конфліктів. І, якщо в лівійській операції, за даними спеціалістів, вони відігравали допоміжну роль, то за відставку Хосні Мубарака в Єгипті топ-менеджер близькосхідного відділення компанії Google Ваел Гонім дякує соціальній мережі Facebook. І на питання, в якій країні вслід за Єгиптом розпочнеться наступна революція радить "запитати в Facebook" [12].

В Україні ж політичне маніпулювання інформацією, що реалізується через мережу Інтернет і, безпосередньо, через соціальні мережі, мережеві співтовариства, може стати серйозною загрозою, як головним засадам розбудови демократичного суспільства і зміцненню незалежності України, так і національній інформаційній безпеці держави. Відповідно, нині існуюча практика використання соціальних мереж із застосуванням специфічних маніпулятивних технологій в умовах зростаючої активізації глобальних процесів у сучасному світі дає підстави для низки висновків.

По-перше, додаткової вразливості національний інформаційний простір набуває через суттєве відставання діючої правової бази від реально існуючих інформаційних процесів у суспільстві. В зв'язку з цим, необхідна організація постійної роботи по приведенню у відповідність правових актів із розвитком інформаційних технологій, забезпечення співмірності цих актів з еволюцією міжнародного законодавства в даній сфері діяльності та зростаючими суспільними потребами, пов'язаними із реалізацією державної програми інформатизації. Важливим також є вдосконалення нормативно-правової бази забезпечення загальнодержавної системи інформаційної безпеки стосовно визначення порядку поширення та використання інформаційної продукції зарубіжного виробництва на території України, врахування вимог інформаційної безпеки при закупівлі зарубіжних програмно-технічних і телекомунікаційних засобів, їх використання в стратегічно важливих галузях, на об'єктах важливого державного та суспільного значення.

По-друге, соціальні мережі надають досить великі можливості для аналізу та прогнозування розвитку подій. Саме тому, венчурний

фонд ЦРУ In-Q-Tel виділяє фінансування не лише на Facebook [13], а й на моніторинг інших соціальних медіа [14]. Такі джерела інформації, зазвичай, досить динамічні: є постійні учасники, є випадкові та періодичні відвідувачі. Проте, коментування всіх новин і подій здійснюється в реальному часі. Відповідно, моніторинг та аналіз таких коментарів дозволяє отримувати зворотній зв'язок і прогнозувати реакцію людей на ті чи інші події, а також знаходити і випробувати нові способи впливу та моделювати ситуації. Таким чином, має здійснюватись оперативне реагування на спроби формування негативного іміджу стосовно України та її громадян, органів державного управління, інших суспільних інститутів, викривлення та тенденційний підбір фактів історичного минулого, поширення неправдивої інформації.

По-третє, організація протидії негативним впливам при використанні соцмереж, зважаючи на їх прискорений розвиток, має ввійти в число основних національних пріоритетів у заходах, орієнтованих на забезпечення вітчизняної інформаційної безпеки. Вона повинна сприяти захисту економічного і політичного суверенітету, власної соціокультурної ідентичності при досягненні балансу між відкритістю інформації, як вимогою сучасного демократичного суспільства, та суспільно необхідними обмеженнями на її поширення.

Організація протидії негативним інформаційним впливам, пов'язаним із використанням соціальних мереж, має сприяти інформаційній діяльності, спрямованій на патріотичне виховання всіх категорій населення, утвердження загальнодержавної системи духовних цінностей, пропаганду толерантності, злагоди, міжрелігійного та міжрелігійного миру, суспільної солідарності. Така робота є особливо важливою у зв'язку із специфікою даного виду інформаційних обмінів на рівні горизонтальних зв'язків між членами суспільства.

Практика функціонування соціальних мереж в останні місяці актуалізує необхідність розробки ефективних технологій для нейтралізації діяльності іноземних політичних, економічних, військових, розвідувальних структур, спрямованої проти інтересів України, в запобіганні проявам інформаційно-диверсійної діяльності терористичних організацій, груп, окремих осіб з метою дестабілізації суспільного життя в країні та завдання шкоди громадянам, державі, введення в систему інформаційних ресурсів спеціально організованої, неправдивої інформації, застосування негативного інформаційно-психологічного впливу на особу.

Сьогодні, саме системний підхід до проблеми організації інформаційної безпеки, формування загальнонаціональної інформаційної системи, скоординованої в своїй діяльності державою, може стати запорукою нейтралізації сучасних інформаційних загроз, у тому числі в сфері розвитку соціальних мереж, використання позитивних факторів розвитку інформатизації в національних інтересах.

Список використаних джерел

1. Петрик В. Небезпеки інформаційного простору для особистості [Електронний ресурс] / В. Петрик // Українські підручники. – Режим доступу : http://pidruchniki.ws/18990227/politologiya/nebezpeki_informatsiyного_prostoru_dlya_osobistosti.
2. Почепцов Г. Г. Інформаційна політика : навч. посіб. / Почепцов Г. Г., Чукут С. А. – [2-ге вид., стер.]. – К. : Знання, 2008. – 663 с.
3. Даниленко С. І. Громадянський вимір інформаційно-комунікаційної революції: концептуально-теоретичні та політико-прикладні аспекти : автореф. дис. ... д-ра політ. наук : 23.00.03 [Електронний ресурс] / С. І. Даниленко ; Київ. нац. ун-т ім. Т. Шевченка. – К., 2011. – 36 с. – Режим доступу : <C:\DOCUME~1\9555~1\LOCALS~1\Temp\11D SIPPA.zip>.
4. Готун А. М. Нові інформаційно-комунікаційні технології в глобальній системі політичної комунікації : автореф. дис. канд. політ. наук : 23.00.04 / А. М. Готун ; Ін-т світ. економіки і міжнар. відносин НАН України. – К., 2010. – 17 с.
5. Маліс О. В. Розвиток Інтернету як комунікативного засобу та його вплив на діяльність суб'єктів політичного процесу в Україні : автореф. дис. ... канд. політ. наук : 23.00.02 / О. В. Маліс ; Ін-т держави і права ім. В. М. Корецького НАН України. – К., 2009. – 19 с.
6. Пілат Є. Феномен соціальних мереж як фактор розвитку громадянського (інформаційного) суспільства й активізації модернізаційних процесів у сфері державного управління [Електронний ресурс] / Є. Пілат // Вісник Львів. ун-ту. Серія юридична. – 2012. – Вип. 56. – С. 180–186. – Режим доступу : http://archive.nbuv.gov.ua/Portal/Soc_Gum/Vlu_yu/2012_56/180con56.pdf.
7. Шестаков В. І. Визначення характеристик інформаційного впливу на складові інформаційно-телекомунікаційних систем в умовах інформаційного протистояння / Шестаков В. І., Чернишук С. В. // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. – Житомир : ЖВІ НАУ, 2011. – Вип. 4. – С. 162–167.
8. Петрик В. Сугестивні технології маніпулятивного впливу [Електронний ресурс] / В. Петрик // Українські підручники – Режим доступу : http://pidruchniki.ws/10590719/psihologiya/sugestiya_internet_informatsiyно-komunikativni_peredumovi.
9. Економічна інформатика : підручник / [Макарова М. В., Гаркуша С. В., Білоусько Т. М., Гаркуша О. В.] ; за заг. ред. д.е.н., проф. М. В. Макарової. – Суми : Університетська книга, 2011. – 480 с.
10. Социальные сети побеждают поисковиков [Электронный ресурс]. – Режим доступа : <http://chip.com.ua/854408.html>.
11. Смола Л. Є. Детермінанти політичного процесу сучасності: теоретико-методологічний аналіз в інформаційно-психологічному вимірі / Л. Є. Смола. – К. : Видавничий дім Дмитра Бураго, 2010. – 243 с.
12. Волошин В. За революцію в Єгипті поборолі Facebook [Електронний ресурс] / В. Волошин // Комсомольская правда. – Режим доступа : <http://www.kp.ru/daily/25637/801883/>.
13. Webre A. L. Facebook [Electronic resource] / A. L. Webre. – Mode of access : http://www.bibliotecapleyades.net/sociopolitica/sociopol_internetfacebook01.htm.
14. Shachtman N. Exclusive: U. S. Spies buy stakes in firm that monitors blogs, tweets [Electronic resource] / N. Shachtman – Mode of access : <http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm/>.

В статье тезисно рассматриваются основные проблемы, связанные с актуализацией проблем информационной безопасности, в связи с растущей ролью социальных сетей в процессе развития информатизации украинского общества.

The article is devoted to the basic issues concerning the information security problems updating, due to the growing role of the social networks in the process of the development of the Ukrainian society informatization.

Стаття надійшла до редакції журналу 24 квітня 2014 року.